VMware Carbon Black EDR

Release Notes: Mac Sensor v6.3.0

May 2020

Summary

VMware Carbon Black EDR macOS Sensor v6.3.0 introduces delivery as an application, fixes a bug regarding MD5 hashing, updates 3rd party SQLite and provides other stability improvements. This sensor release also includes all changes and fixes from previous releases.

This document provides information for users upgrading to VMware Carbon Black EDR macOS Sensor v6.3.0 from previous versions as well as users new to VMware Carbon Black EDR. The key information specific to this release is provided in the following major sections:

- **Installation Instructions** - Provides instructions for VMware Carbon Black EDR macOS sensor installation.
- **New features** – Describes new features introduced in this release.
- **Corrective content** – Describes issues resolved by this release as well as more general improvements in performance or behavior.
- **Known issues and limitations** – Describes known issues or anomalies in this version that you should be aware of.

Server compatibility

VMware Carbon Black EDR sensors included with server releases are compatible with all server releases going forward. It is always recommended to use the latest server release with our latest sensors to utilize the full feature capabilities of our product, however, using earlier server versions with the latest sensor should not impact core product functionality.

Sensor operating systems

VMware Carbon Black EDR sensors interoperate with multiple operating systems. For the most up-to-date list of supported operating systems for VMware Carbon Black EDR sensors (and all VMware Carbon Black products), refer to the following location in the VMware Carbon Black User eXchange: https://community.carbonblack.com/docs/DOC-7991

Documentation

This document supplements other VMware Carbon Black documentation. Click here to search the full library of VMware Carbon Black EDR user documentation on the VMware Carbon Black User eXchange.

Technical support

VMware Carbon Black EDR server and sensor update releases are covered under the Customer Maintenance Agreement. Technical Support is available to assist with any issues that might develop during the installation or upgrade process. Our Professional Services organization is also available to assist to ensure a smooth and efficient upgrade or installation.

Carbon Black, Inc. | 1100 Winter Street, Waltham, MA 02451 USA | Tel: 617.393.7400

Note: Before performing an upgrade, VMware Carbon Black recommends reviewing content on the User eXchange for the latest information that supplements the information contained in this document.

Installation Instructions

To install the sensors on to your server, run through the following instructions:

1. Ensure your VMW CB EDR YUM repo is set appropriately:
    a. The VMW CB EDR repository file to modify is */etc/yum.repos.d/CarbonBlack.repo*
    b. Baseurl = https://yum.distro.carbonblack.io/enterprise/stable/$releasever/$basearch/
2. On the VMW CB EDR server, clear the YUM cache by running the following command:
    a. yum clean all
3. After the YUM cache has been cleared, download the sensor install package by running the following command:
    a. Run *yum install --downloadonly --downloaddir=<package local download directory> <package>*
        i. **Note:** The *<package local download directory>* is a directory of your choice
        ii. **Note:** *<package>* is replaced by *cb-osx-sensor*
4. Install the new sensor package on the VMW CB EDR server by running the command:
    a. rpm -i --force <package>
5. Make the new installation package available in the server console UI by running the command:
    a. /usr/share/cb/cbcheck sensor-builds --update
        i. **Note:** If your groups have *Automatic Update* enabled, the sensors in that group will start to automatically update.

Your new sensor versions should now be available via the console. For any issues, please contact VMware Carbon Black Technical Support.

New Features

- **Sensor delivery as an application** – The macOS sensor will be delivered as an application (bundle) starting with v6.3.0 and will be stored in the applications directory. While kernel extensions will still be used in v6.3.0, delivery as a bundle application is required to run system extensions in future sensor releases. [CB-28759]

Corrective Content

This release provides the following corrective content changes:

- Fixed bug with MD5 hashing related to race conditions when calling *mmap* function. [CB-17695]

Known Issues and Limitations

Known issues associated with this version of the sensor are included below:

- This release has an updated path directory and daemon. Host checks (where applicable) will need to be updated to reflect this. The new installation path is /Applications/VMware Carbon Black EDR.app/. More information is available at the UeX post here.

  Additionally, our daemon was renamed to /Applications/VMware Carbon Black EDR.app/Contents/MacOS/CbOsxSensorService.

- After downgrading from a 6.3.x sensor version to a 6.2.x sensor version, the application icon remains in the */Applications* directory and is visible to the user. Clicking the icon produces no action. The icon can be deleted manually with no ill-effects. See our Knowledge Base here for more information.

- Downgrading from v6.3.0 on an endpoint with a version of macOS 10.13+ installed will require a reboot on the downgraded endpoint due to OS requirement changes with kext approval introduced in macOS 10.13 High Sierra. More information is available at the UeX post here.

- Downgrading manually from v6.2.7+ to v6.2.6 and previous sensor versions will require a reinstallation due to changes in the way the sensor database is accessed. More information can be found at the UeX post here. [CB-28154]

- The Original Filename and Product Name for the CommCenter binary on MacOS is not being properly captured in the Server UI. [CB-17611]

- If you disable path exclusions in *cb.conf* you must reboot the system to update the previous path exclusion settings preserved in cache. [CB-14660]

- The Mac Response sensor does not store Live Response activity in the *sensor.log* file by default. Users can monitor Live Response activity using the *live-response.log* found under */var/log/cb/audit* on the Response server. Additionally, users can enable more verbose logging of the *sensor.log* file to capture Live Response activity on the Mac endpoint. **Please note**, enabling verbose logging may quickly consume the specified

sensor.log size and should be used cautiously as enabling may lead to shorter retention of audit information. This verbose logging can be enabled by modifying the *logging.config* file under */var/lib/cb* to to set the following parameters: *minloglevel: 0*, *V:0*. [CB-8908]

Contacting Support

Use one of the following channels to request support or ask support questions:

- **Web:** User eXchange
- **Email:** support@carbonblack.com
- **Phone:** 877.248.9098
- **Fax:** 617.393.7499

Reporting Problems

When contacting VMware Carbon Black Technical Support, be sure to provide the following required information about your question or issue:

- **Contact:** Your name, company name, telephone number, and email address
- **Product version**: Product name (VMware Carbon Black EDR server and sensor version)
- **Hardware configuration:** Hardware configuration of the VMware Carbon Black EDR server (processor, memory, and RAM)
- **Document version:** For documentation issues, specify the version and/or date of the manual or document you are using
- **Problem:** Action causing the problem, error message returned, and event log output (as appropriate)
- **Problem severity:** Critical, serious, minor, or enhancement request